

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

**Listing of Claims:**

This listing of claims replaces all prior versions and listings of claims in the application.

**Listing of Claims**

1. (currently amended) An unsolicited message rejecting communications processor connected to between message transfer agents MTA\_0 with an Internet address of IP\_0, a from-address A\_0, a declared domain of D\_0, and actual a real domain of DD\_0, and MTA\_1 with an Internet address of IP\_1, a domain D\_1, and a to-address A\_1 comprising:
  - a) monitoring means for monitoring the communications between MTA\_0 and MTA\_1;
  - b) determining means for determining if the communications contains a message that is an unsolicited message; and
  - c) intercepting means for intercepting a .\r\n end-of-message indicator reply from MTA\_0, forcing MTA\_0 to QUIT its connection with MTA\_1 the unsolicited message rejecting communications processor by sending an error reply to MTA\_0 if the message is determined to be unsolicited[[.]]; whereby MTA\_1 controls the interaction wherein the unsolicited message rejecting communications processor does not intercept communications between MTA\_0 and MTA\_1 before a .\r\n end-of-message indicator reply from MTA\_0 is received by the unsolicited message rejecting communications processor.

2. (currently amended) The unsolicited message blocking rejecting communications processor in Claim 1, further includes a an allow\_address

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

database and wherein the determining means determines if at the message is not unsolicited by checking if the IP\_0 is in the allow\_address database.

3. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes a prevent\_address database and wherein the determining means determines if at the message is unsolicited by checking if IP\_0 is in the prevent\_address database.

4. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes access to a/an open relay database and wherein the determining means determines if at the message is unsolicited by checking if IP\_0 is in the open relay database.

5. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes access to a DNS (domain name server) database and wherein the determining means determines if at the message is unsolicited by checking if IP\_0 has a domain name entry DD\_0 in the DNS database.

6. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes a bad\_from database and wherein the determining means determines if at the message is unsolicited by checking if the from-address A\_0 is in the bad\_from database.

7. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes a suspect\_domain database and wherein the determining means determines if at the message is unsolicited by checking if the actualreal domain DD\_0 matches the domain of the from-address A\_0 and the domain of the from-address A\_0 is in the suspect\_domain database.

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

8. (currently amended) The unsolicited message ~~blocking~~rejecting communications processor in Claim 1, wherein the determining means determines if ~~at~~the message is unsolicited by checking if the from-address A\_0 matches the to-address {A\_1}.
9. (currently amended) The unsolicited message ~~blocking~~rejecting communications processor in Claim 1, further includes a no\_filter database and wherein the determining means determines if the message is to be blocked if it is determined to be unsolicited.
10. (currently amended) The unsolicited message ~~blocking~~rejecting communications processor in Claim 1, wherein the determining means determines if a message is unsolicited by checking if the declared domain D\_0 of MTA\_0 is the same as the domain D\_1 of MTA\_1.
11. (currently amended) The unsolicited message ~~blocking~~rejecting communications processor in Claim 1, wherein the determining means determines if a message is unsolicited by checking if the declared domain D\_0 of MTA\_0 does not match the real domain DD\_1DD\_0 and the declared domain D\_0 is in the suspect\_domain database.
12. (currently amended) The unsolicited message ~~blocking~~rejecting communications processor in Claim 1, further includes a bad\_word database and wherein the determining means determines if ~~at~~the message is unsolicited by checking if the subject line of the message contains any words in the bad\_word database.
13. (currently amended) The unsolicited message ~~blocking~~rejecting communications processor in Claim 1, further includes a bad\_fingerprint

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

database and wherein the determining means determines if the hash "fingerprint" of a portion of the body of the message is in the bad\_fingerprint database.

14. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes a rejected\_connection database which logs the time, from-address A\_0, to-address A\_1, and the reason for the rejection if the message is rejected if the message is determined to be unsolicited.

15. (currently amended) The unsolicited message blockingrejecting communications processor in Claim 1, further includes an allowed\_connection database which logs the time and to-address A\_1 if the message is determined not to be unsolicited.

16. (currently amended) A method for

a receiving networked computer system with an Internet connection, a ~~mail transport~~message transfer agent MTA\_1, an Internet address IP\_1, a to-address A\_1, and an operating system capable of executing the method

to reject unsolicited messages from

a transmitting networked computer system with an Internet connection and a message transfer agent MTA\_0, an Internet address IP\_0, a from-address A\_0, a declared domain D\_0, and actual a real domain DD\_0

comprising the steps of:

- a) waiting for a new SMTP connection request;
- b) relaying and monitoring the replies from MTA\_0 to MTA\_1;
- c) relaying replies from MTA\_1 to MTA\_0;
- d) intercepting the .\r\n end-of-message indicator reply from MTA\_0 to MTA\_1;

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

- e) determining if the message is unsolicited by analyzing the monitored replies;
- f) releasing the intercepted .\r\n end-of-message reply if the message is determined not to be unsolicited; and
- g) sending an error reply to MTA\_0 to force MTA\_0 and MTA\_1 to close down their connection;

whereby MTA\_1 controls the interaction between MTA\_0 and MTA\_1 until a .\r\n end-of-message indicator reply is received from MTA\_0.

17. (currently amended) A method for

a receiving networked computer system with an Internet connection, a DNS server, and an open relay database, a mail transport message transfer agent MTA\_1, an IP address IP\_1, a domain name D\_1, a recipientto-address[.] A\_1, an allow\_address database, a prevent\_address database, a suspect\_domain database, a bad\_from database, a no\_filter database, a yes\_filter database, a bad\_word database, a bad\_fingerprint, a rejected\_connection database, an allowed\_connection database, and an operating system capable of executing the method

to reject unsolicited messages from

a transmitting networked computer system with an Internet connection, a message transfer agent MTA\_0, an IP address of IP\_0, a declared domain name D\_0, a real domain name DD\_0, and a sender addressfrom-address of A\_0

comprising the steps of:

- a) waiting for a SMTP connection request on the receiving networked computer system's Internet connection;
- b) sending a 220 reply to MTA\_0 to acknowledge the requested connectionSMTP connection request;

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

- c) extracting the IP address IP\_0 from the connection request~~SMTP connection request~~;
- d) requesting at~~the~~ domain name DD\_0 for IP\_0 from the DNS server;
- e) testing if the domain name DD\_0 is "no name";
- f) testing if IP\_0 is in an~~the~~ open relay database;
- g) testing if IP\_0 is in the allow\_address database;
- h) testing if IP\_0 is in the prevent\_address database,
- i) requesting a connection with MTA\_1;
- j) waiting for a 220 reply from MTA\_1 to acknowledge the requested connection;
- k) waiting for a reply from either MTA\_0 or MTA\_1;
- l) jumping to step o) if the reply is not from MTA\_1;
- m) relaying the reply from MTA\_1 to MTA\_0;
- n) jumping to step k) to wait for a new reply;
- o) jumping to step u) if the reply from MTA\_0 is not a **HELO**;
- p) extracting the declared domain D\_0 from the reply;
- q) testing if the declared domain D\_0 ~~of MTA\_0~~ matches the domain D\_1 ~~of MTA\_1~~;
- r) testing if the declared domain D\_0 does not match the real domain DD\_0 ~~of MTA\_0 AND the declared domain D\_0 is in the suspect\_domain database;~~
- s) relaying the HELO reply from MTA\_0 to MTA\_1;
- t) jumping to step k) to wait for a new reply;
- u) jumping to step aa) if reply from MTA\_0 is not a **MAIL**;
- v) extracting the from-address A\_0;
- w) testing if A\_0 is in the bad\_from database;
- x) testing if DD\_0 does not match the domain of A\_0 and the domain of A\_0 is in the suspect\_domain database;
- y) relaying MAIL reply to MTA\_1;
- z) jumping to step k) to wait for a new reply;

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

- aa) jumping to step ii) if the reply from MTA\_0 is not a **RCPT**;
- bb) extracting the to-address A\_1;
- cc) testing if A\_1 is in the no\_filter database;
- dd) testing if A\_0 matches A\_1;
- ee) testing if A\_0 is in the no\_filter database;
- ff) testing if A\_0 is in the yes\_filter database;
- gg) relaying RCPT reply to MTA\_1;
- hh) jumping to step k) to wait for a new reply;
- ii) jumping to step yy) if the reply from MTA\_0 is not **DATA**;
- jj) relaying DATA to MTA\_1;
- kk) waiting for a\_354 reply from MTA\_1;
- ll) relaying a\_343 reply to MTA\_0;
- mm) wait for the body of the message;
- nn) relaying the body of the message to MTA\_1;
- oo) waiting for a .\r\n end-of-message indicator;
- pp) testing if any word in the subject line of the message is in the bad\_word database;
- qq) testing if the hash "fingerprint" of a portion of the message is in the bad\_fingerprint database;
- rr) jumping to step vv) if NOT(t\_allow OR t\_no\_filter OR OR NOT t\_yes\_filter OR NOT ( t\_prevent OR t\_open OR t\_DD-) OR t\_bad\_from OR t\_suspect\_domain OR t\_echo\_domain OR t\_forged\_domain OR t\_bad\_word OR t\_bad\_fingerpring)) ;
- ss) logging the time and the to-address A\_1 in the allowed\_connection database;
- tt) relaying the .\r\n end-of-message indicator reply to MTA\_1 to continue the conversation;
- uu) jumping to step k) to wait for a new reply;
- vv) logging the time, the from-address A\_0, the to-address A\_1, and the reason for rejecting the connection in the rejected\_connection database;

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

- ww) sending a 554 reply to MTA\_0 to terminate the conversation;
- xx) jumping to step k) to wait for a new reply;
- yy) jumping to step ggg) if the reply from MTA\_0 is not **RSET, SEND, SCML, SAML, VRFY, NOOP, EXPN, HELP, or TURN**;
- zz) relaying the reply to MTA\_1;
- aaa) jumping to step j) to wait for a new reply;
- bbb) jumping to step ddd) if the reply from MTA\_0 is not a **QUIT**;
- ccc) relaying the QUIT reply to MTA\_1;
- ddd) waiting for a221 reply from MTA\_1
- eee) relaying a221 reply from MTA\_1 to MTA\_0;
- fff) jumping to step a) to wait for a new connection;
- ggg) sending a 500 reply to MTA\_0 to signal a syntax error; and
- hhh) jumping to step a) to wait for a new connection.

18. (new) A method comprising:

- a) relaying and monitoring SMTP messages exchanged between a transmitting message transfer agent (MTA\_0) and a receiving message transfer agent (MTA\_1);
- b) intercepting a .\r\n end-of-message indicator reply from MTA\_0;
- c) determining if an e-mail message is unsolicited by analyzing the monitored SMTP messages; and
- d) releasing the .\r\n end-of-message indicator reply if the message is determined not to be unsolicited, whereas, sending an error reply to MTA\_0 to force MTA\_0 to close its communications connection if the message is determined to be unsolicited.

19. (new) An apparatus comprising:

- a communications port; and
- means for

Applicants: White et al.  
Serial No.: 10/761,894  
Filing Date: January 20, 2004  
Docket No.: EGT-006-1C

- a) relaying and monitoring SMTP messages exchanged between a transmitting message transfer agent (MTA\_0) and a receiving message transfer agent (MTA\_1);
- b) intercepting a .\r\n end-of-message indicator reply from MTA\_0;
- c) determining if an e-mail message is unsolicited by analyzing the monitored SMTP messages; and
- d) releasing the .\r\n end-of-message indicator reply if the message is determined not to be unsolicited, whereas, sending an error reply to MTA\_0 to force MTA\_0 to close its communications connection if the message is determined to be unsolicited.